UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/942,633	08/30/2001	Steven Black	AUS920010244US1	8760

7590 06/23/2005

Duke W. Yee
Carstens, Yee & Cahoon, LLP
P.O. Box 802334
Dallas, TX 75380

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 06/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/942,633	BLACK ET AL.	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 March 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) 8-10, 18-20 and 28-30 is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,11-17 and 21-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *02/04/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Response to Arguments

1. This communication is in response to applicants' response received on March 15, 2004.

2. Claims 8-10, 18-20 and 28-30 are withdrawn from further consideration pursuant to 37 CFR 1.142(b), as being drawn to a nonelected invention, there being no allowable generic or linking claim. Applicant timely traversed the restriction (election) requirement in the reply filed on March 15, 2004.

3. Applicants' election with traverse of claims 1-7, 11-17 and 21-27 in the reply filed on March 15, 2004 is acknowledged. The traversal is on the ground that claims 1 and 8 do not have separate utility. A reply to the traversal appears below.

The requirement is still deemed proper and is therefore made FINAL.

4. Applicants argue on page 11 of the remark that "...claims 1 and 8 do not have separate utility" and "moreover, claim 8 is not understandable without the disclosure related to claim 1."

Claim 1 invention claims a method for reporting security situation that comprises calculation of delta severities from severity levels and propagating it to a higher-level correlation server in addition to logging and classifying of events. These functions are different with what claim 8 invention claims. Because claim 8 invention claims a method of establishing a severity level for multiple groups of computers comprising the receipt

of delta severity levels and performing mathematical operations on them. If the data processing system is the top level of a hierarchy of servers, also a second mathematical operation would be performed on the new delta severity level. The details of logging and classifying as recited in claim 1 are not found in claim 8. Likewise the details of establishing a severity level of claim 8 are not recited in claim 1. As such, the invention of claim 8 has separate utility apart from the invention of claim 1, since establishing severity levels as recited in claim 8 may be used in a display of threats rather than a logging and classifying system as recited in claim 1.

4. In light of the above submission, the restriction requirement is maintained and only the claims of Group I are be examined as follows.

Claim Rejections - 35 USC § 102

> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-7, 11-17 and 21-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Molini et al (6,353,385; hereinafter Molini).

Regarding claims 1, 11 and 21, Molini discloses:

logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute (see for example, col. 5, lines 1-10; col. 7, lines 1-6; col. 9, lines 24-29);

classifying events as groups by aggregating events with at least one attribute within the event set as an identical value (see for example, col. 8, lines 25-37; col. 7, lines 19-20; col. 6, lines 49-51; col. 9, lines 30-35);

calculating severity levels for the groups (see, for example, col. 7, lines 50-60; col. 7, lines 27-33);

calculating delta severities from the severity levels (see, for example, col. 6, lines 52-62; col. 6, lines 15-21, where the highest priority alarm corresponds to the recited delta severity); and

propagating the delta severities to a higher-level correlation server (see, for example, col. 3, lines 46-59; col. 6, lines 18-37, where the central station corresponds to the recited higher-level correlation server).

Regarding claims 2, 12 and 22, Molini discloses:

The method of claim 1, wherein the severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of

the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups (see, for example, col. 7, lines 27-40; col. 8, lines 48-55).

Regarding claims 3, 13 and 23, Molini discloses:

The method of claim 1, wherein the events include at least one of a web server event, an electronic mail event, a Trojan horse, denial of service, a virus, a network event, an authentication failure, and an access violation (see, for example, col. 1, lines 60-62; col. 3, lines 36-38, where attack over Internet on a protected computer corresponds to the recited events).

Regarding claims 4, 14 and 24, Molini discloses:

The method of claim 1, further comprising: calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group (see, for example, col. 7, lines 50-63; col. 8, lines 48-55).

Regarding claims 5, 15 and 25, Molini discloses:

The method of claim 1, wherein the target attribute represents one of a computer and a collection of computers (see, for example, col. 1, lines 29-35).

Regarding claims 6, 16 and 26, Molini discloses:

The method of claim 1, wherein the source attribute represents one of a computer and a collection of computers (see, for example, col. 1, lines 29-35).

Regarding claims 7, 17 and 27, Molini discloses:

The method of claim 1, further comprising: aggregating a subset of the groups into a combined group (see, for example, col. 9, lines 30-36).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Patent No. 6,553,378 B1 to Eschelbeck.

US Patent Pub. No. 2002/0138571 A1 to Trinon et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar
Examiner
Art Unit 2132

AN
June 16, 2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100